Claims

1. A consumable authentication protocol for validating the authenticity of an untrusted authentication chip, the protocol includes the steps of:

generating a secret random number and calculating a signature for the random number using a signature function, in a trusted authentication chip;

encrypting the random number and the signature using a symmetric encryption function using a first secret key, in the trusted authentication chip;

passing the encrypted random number and signature from the trusted authentication chip to an untrusted authentication chip;

decrypting the encrypted random number and signature with a symmetric decryption function using the first secret key, in the untrusted authentication chip;

calculating a signature for the decrypted random number using the signature function in the untrusted authentication chip;

comparing the signature calculated in the untrusted authentication chip with the signature decrypted;

in the event that the two signatures match, encrypting the decrypted random number together with a data message read from the untrusted chip by the symmetric encryption function using a second secret key and returning it together with the data message to the trusted authentication chip;

encrypting the random number together with the data message by the symmetric encryption function using the second secret key, in the trusted authentication chip;

comparing the two versions of the random number encrypted together with the data message using the second key, in the trusted authentication chip;

in the event that the two versions match, considering the untrusted authentication chip and the data message to be valid;

otherwise, considering the untrusted authentication chip and the data message to be invalid.

2. A consumable authentication protocol according to claim 1, where the two secret keys are held in both the trusted and untrusted chips and are kept secret.

3. A consumable authentication protocol according to claim 1, where the random number is generated from an initial seed value only in the trusted chip, and the seed value is changed for generating a new random number only after each successful validation.

4. A consumable authentication protocol according to claim 1, where the data message is a memory vector of the authentication chip.

5. A consumable authentication protocol according to claim 4, where part of the vector space is different for each chip, part of it is constant (read only) for each consumable, and part of it is decrement only.

6. A consumable authentication protocol according to claim 1, where the encryption function is held in both chips.

7. A consumable authentication protocol according to claim 1, where the decryption function is held only in the untrusted chip.

8. A consumable authentication protocol according to claim 1, where the signature function is held in both chips to generate digital signatures.

9. A consumable authentication protocol according to claim 8, where the digital signature is between 128 bits and 160 bits long, inclusive.

10. A consumable authentication protocol according to claim 1, where a test function is held only in the trusted chip to return an indication that the untrusted chip is valid and advance the random number, if the untrusted chip is valid; otherwise it returns an indication that the untrusted chip is invalid.

11. A consumable authentication protocol according to claim 10, where the time taken to return an indication that the untrusted chip is invalid is identical for all bad inputs, and the time taken to return an indication that the untrusted chip is valid is identical for all good inputs.

12. A consumable authentication protocol according to claim 1, where a read function in the untrusted chip decrypts the random number and signature, calculates its own signature for the decrypted random number and compares the two signatures, then it returns the data message and a reencrypted random number in combination with the data message if the locally generated signature is the same as the decrypted signature; otherwise it returns an indication that the untrusted chip is invalid.

13. A consumable authentication protocol according to claim 12, where the time taken to return the invalid indication is identical for all bad inputs, and the time taken to make a return for a good input is the same for all good inputs.

14. A consumable authentication system for performing the method according to claim 1; where the system includes a trusted authentication chip and an untrusted authentication chip; the trusted authentication chip includes a random number generator, a symmetric encryption function and two secret keys for the function, a signature function

and a test function; and the untrusted authentication chip includes symmetric encryption and decryption functions and two secret keys for these functions, a signature function and a read function to test data from the trusted chip, including a random number and its signature, encrypted using the first key, by comparing the decrypted signature with a signature calculated from the decrypted random number, and in the event that the two signatures match, to return a data message and an encrypted version of the data message in combination with the random number, encrypted using the second key; the test function operates to encrypt the random number together with the data message by the symmetric encryption function using the second secret key, compare the two versions of the random number encrypted together with the data message using the second key, and in the event that the two versions match, considers the untrusted authentication chip and the data message to be valid, otherwise, it considers the untrusted authentication chip and the data message to be invalid.

15. A consumable authentication system according to claim 14, where the two secret keys are kept secret.

16. A consumable authentication system according to claim 14, where the random number is generated by the random number generator from an initial seed value only in the trusted chip, and the seed value for generating a new random number is changed only after each successful validation.

17. A consumable authentication system according to claim 14, where the data message is a memory vector of the authentication chip.

18. A consumable authentication system according to claim 17, where part of the vector space is different for each chip, part of it is constant (read only) for each consumable, and part of it is decrement only.

19. A consumable authentication system according to claim 14, where the signature function operates to create digital signatures between 128 bits and 160 bits long.

20. A consumable authentication system according to claim 14, where the test function advances the random number in the event of a match.

21. A consumable authentication system according to claim 14, where the time taken for the test function to return an indication that the untrusted chip is invalid is identical for all bad inputs, and the time taken to return an indication that the untrusted chip is valid is identical for all good inputs.

22. A consumable authentication system according to claim 14, where the time taken for the read function to return the invalid indication is identical for all bad inputs, and the time taken to make a return for a good input is the same for all good inputs.

SUBSTITUTE SHEET (RULE 26)